Regular, Fast, Ultrafast Ethernet

10Base5 – “Thick Ethernet or Thicknet” – is the original Institute of Electronic and Electrical Engineers (IEEE) 802.3 Ethernet.

10Base2 – “Thin Ethernet, Thinnet, or Cheapernet” – resembles 10Base5, was introduced to reduce the cost and complexity of installation, and became very popular for replacing Thick Ethernet as an office-cabling solution.

10Base-T, an IEEE 802.3i physical later that uses two pairs of unshielded twisted-pair (UTP) telephone-type cable: one to Transmit; the other to Receive.

10Base-F refers to 3 different fiber-optic specifications:
- 10Base-FL (Fiber Link) replaced the 1987 Fiber Optic Inter-Repeater Link (FOIRL) Specification and is backward compatible with existing FOIRL devices. It is the most popular 10Mbps fiber standard.
- 10Base-FP and 10Base-FB are dead. P means passive; B means backbone.

Fast Ethernet 10Base-T is 10Base-T with original Ethernet Media Access Controller (MAC) at 10 times the speed. It allows three physical-layer implementations, all part of IEEE 802.3u: 100Base-TX has two pairs of Category 5 UTP or Type 1 STP cabling and is most popular for horizontal connections; 100Base-FX has two strands of multi-mode fiber and is popular for vertical or backbone connections; 100Base-T4 has four pairs of Category 3 or better cabling and is not common.

Gigabit or 1000Mbps Ethernet is the 1998 IEEE 802.3z standard that includes the Gigabit Ethernet MAC and three physical layers. Gigabit uses 8B/10B encoding and encompasses three physical standards: 1000Base-SX Fiber (horizontal fiber), 1000Base-LX Fiber (vertical or campus backbone), 1000Base-CX Copper (Copper-Twinax cabling), and 1000Base-T.

What Means What?
The IEEE naming convention for Ethernet is:

- The first number (10, 100, 1000) indicates the transmission speed in megabits per second (mbps).
- The second term indicates transmission type: Base = baseband; BROAD = broadband.
- The last number indicates segment length. 5 means a 500-meter (500-m) segment length from original Thicknet.

In newer IEEE standards, letters replace numbers. For example, in 10Base-T, the T means unshielded twisted-pair cables; in 100Base-T4, the T4 indicates four such pairs.

7 Layer Network Concept
[Adapted from Sensors Magazine, July 2001 ©Advantstar]

For many years, the ISO/OSI model described the layers of information in a network, particularly the low-level transport mechanisms. From top to bottom, these are the layers and how these layers relate to your product design:

<table>
<thead>
<tr>
<th>Layer</th>
<th>Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
<td>Meaning of data</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
<td>Building blocks of data and encryption</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
<td>Opening and closing of specific communication paths</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
<td>Error checking</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
<td>Determination of data paths within the network</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
<td>Data transmission, source, destination, and checksum</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
<td>Voltage levels, signal connections, wire, or fiber</td>
</tr>
</tbody>
</table>

Most networks do not use all layers. For example, Ethernet and RS-232 are physical layers: layer 1 only for RS-232; layers 1 and 2 for Ethernet. TCP/IP is a protocol, not a network, and uses layers 3 and 4 regardless of whether layers 1 and 2 are a telephone line, wireless connection, or 10Base-T Ethernet cable.
Ethernet Network Design Rule

The “5-4-3-2” rule states that the maximum transmission path is composed of 5 segments linked by 4 repeaters and, at most, the segments can be made of 3 coaxial segments with station nodes and 2 link [10Base-FL] segments with no nodes between. Exceeding these rules means that some nodes will be unable to communicate with some other nodes.

Below is a popular simplification of the IEEE 802.3 Rule regarding maximum transmission length between two nodes:

Hub Types: workgroup, usually stand-alone units with four to eight ports; stackable, with many more ports that can be linked to form a “super hub;” segmented which allow available ports to be divided among multiple groups and collision domains; two-speed which allow multiple baud rates to operate on the same hub, auto-detecting the data rate at each port and linking ports together with a speed-matching bridge; managed which have modest levels of intelligence and can be controlled remotely via a configuration port; and repeaters, essentially two-port hubs, which clean up the signal and boost it over distances.

Ethernet Switches route communication to the desired end devices instead of broadcasting the communication to everyone connected to the LAN. This is done by the switch’s ability to set up a table of device addresses connected to each leg of the switch. With this information the switch knows where to send each Ethernet packet once it is received. Switches are plug and play and increase the number of nodes and the length of the LAN. They are designed to divide the network into separate collision domains. This reduces overall traffic on a LAN, improving communication speed and reducing errors.

Managed Switches allow advanced control of your LAN. They usually include software to configure your network and diagnostic ports to monitor LAN traffic. If communications fail, most managed switches will alert the manager via e-mail or by closing a relay to trigger an audible signal or flash a light. Another feature available on managed switches is QoS (Quality of Service) programming which prioritizes messages ensuring important data receives the highest priority on the LAN segment. See Managed Ethernet Switches.

Media Converters change Ethernet twisted-pair copper wires into fiber optic signals. Fiber optic is often preferable because it is impervious to interference that can disrupt the signals being carried by copper. Because fiber can extend the distance of a network up to 2 km in each segment, media converters can also increase the range of a network.
Stacking or Crossover Cables allow multiple hubs to be connected in a daisy-chain topology. You cannot use standard cables to link two hubs or two NIC cards together because they link transmit pins to transmit pins instead of transmit pins to receive pins. Note: Some hubs have crossover ports, which allow standard cables to be used.

Bridges, which operate at layer 2 of the OSI model, extend the reach of each segment and allow traffic to selectively pass between two network segments. Bridges make forwarding decisions based on MAC addresses.

Intelligent bridges learn over time what devices are connected on each side and figure out which messages to forward and which ones to block. Such a bridge will automatically adapt to changes made to the networks over time.

Do not form loops on networks with multiple connecting bridges. The IEEE 802.1 spanning-tree algorithm removes loops: One bridge in a loop becomes the root and all other bridges send frames to it. Note: Bridges are not assigned MAC or IP addresses.

Routers, which maintain tables of IP addresses on each segment, learn the most direct paths for sending data packets to their destination. Routers are protocol-dependent because they operate at layer 3. Types include: 2-port; multi-port; access, which use modems; bridging, also called “brouters”, which change from router to bridge when they receive a packet that they do not understand and send the message.

Gateways convert messages from one protocol to another, such as Modbus on RS-232 to Ethernet Modbus/TCP, or DeviceNet to EtherNet/IP. In most cases, the physical layers, protocols, and speeds are different. Gateways must normally be configured to work properly and are temporary rather than permanent solutions. Interface cards (NICs) link the PC to Ethernet via the PCI, ISA, PCMCIA, PC/104, or other buses. NICs handle layers 1 and 2, while the host processor in the PC handles everything else.

Software handles all other network layers, including TCP/IP, which comes built-in to nearly all PC operating systems, including Windows, Linux, DOS, UNIX, VxWorks, etc. Software applications for control or operator interfaces have drivers that pass application data, including higher-layer protocols like Modbus/TCP and EtherNet/IP to TCP/IP.

Driver performance – There are no defined standards for driver performance and there can be significant performance issues and delays with respect to driver and application performance. Many drivers are not written to serve the needs of deterministic applications.

Response time can vary considerably on the basis of CPU speed, memory, how well the drivers are written, what other applications are running on the PC, etc. In most cases, the speed of industrial Ethernet networks will be limited by software and drivers, not by Ethernet itself.

Selecting the Right Cable
Select the right cable – and ensure that all components and interconnects on the network are equal to the cable’s quality level. Grounding coaxial cable is generally good as it dissipates static electricity and makes your network safer. Use fiber optic cables to link buildings, not copper.

Shielded twisted pair (STP) cable is naturally noise immune and preferable to unshielded twisted pair (UTP) in noisy situations. STP should have at least 40 dB CMRR and less than 0.1 pF capacitance unbalance per foot. Ground the STP cable, ensuring the ground is connected only at one end. Cat5 STP patch panels can provide a grounding strip or bar.
Hubs and switches don’t provide grounding—use cables.

It is wise to be conservative about cables’ ability to reject noise from 220 VAC and 440 VAC power lines and noisy power supplies of a factory. Capacitance imbalance greater than 70 pF per 100 m can introduce harmonic distortion, resulting in bit errors.

The cost of cable is quite low compared to total equipment cost. If you are looking to save money, this is not a place to do it. Choose a well-designed cable to minimize bit-error rate after installation for faster throughput and fewer glitches.

Fiber-optic cable – certainly more expensive but bypassing the electrical issues such as noise and harmonic distortion, grounding, etc., especially in high-speed networks – it is a very attractive choice.

If one section of a network is exposed to excess amounts of electrical noise, it is best to isolate that section with switches. But, if you must use a hub in a noisy environment, use one with some level of intelligence instead of a buffer.

If your equipment is subject to washdown or exposure to corrosive chemicals, select cables with insulation that is rated to withstand exposure to those chemicals, such as polyurethane (PUR).

Choosing the Best Network

Ethernet must work with other network technologies and, for some applications, other networks will deliver more cost-effective performance. Ask these question:

- What is the distance requirement?
- What physical cabling arrangement makes sense for this application?
- What is the speed ("response time") requirement for the most time-critical devices? Do all devices require that speed? Should some have a higher priority than others?
- Does the network allow you to prioritize messages?
- Do the devices that you want to use support the same network standard? Are there open versus closed architecture considerations?
- If you are developing a network-capable product, what is the hardware bill of materials and cost of software development for that network?
- How much electrical noise is present in the application and how susceptible is the cabling to such interference?
- What is the maximum required packet size for the data that will be sent? If the data can be fragmented over several packets, how fast does a completed message have to arrive?
- What type(s) of device relationships are desired: master/slave, peer-peer, or broadcast?
- Does the network need to distribute electrical power? If so, how much current?
- What kind of fault tolerance needs to be built into the network architecture?
- What is the total estimated installed cost?